



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,520	10/26/2001	Petr Peterka	018926-006530US	2602

20350 7590 02/15/2006

TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

EXAMINER

BESROUR, SAOUSSEN

ART UNIT PAPER NUMBER

2131

DATE MAILED: 02/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/007,520		PETERKA ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Saoussen Besrouer		2131	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 29 April 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 October 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. This action is in response to preliminary amendment filed 4/29/2003. Claims 13 and 20 were amended. Claims 1-32 are pending.

### *Priority*

2. This application claims priority to Provisional Application Serial No. 60243925, filed 10/26/2000.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 22, 23, 24, 25, 26, 27, 28 and 29** rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al. (U.S. Patent No. 6,385,596) in view of Kandansky et al. (U.S. Patent No. 6,295,361).

As per **claim 1**, Wiser et al. discloses: receiving a request for a key from a client (Column 9, Lines 25-27 and Lines 57); logging said request for said key in a log (Column 18, Lines 23-25); distributing said key to said client in response to said request (Column 9, Lines 27-36); billing said client based upon said log (Column 18, Lines 25-28). Wiser et al. does not explicitly disclose multicasting program content for decryption by said client utilizing said key. Kandansky et al. discloses multicasting program

content for decryption by said client utilizing said key (Column 4, Lines 15-20).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky et al. in conjunction with the teachings of Wiser et al. for the benefit of disseminating data to a large group of receivers in a network (Column 1, Lines 9-10).

As per **claim 22**, Wiser et al. discloses: multicasting encrypted program content (Column 7, Lines 26-45 and Column 9, Lines 25-37); creating a list of active participants receiving said program, said list of active participants including said client (Column 18, Lines 23-29); and receiving a message from said client indicating that said client should remain on said list of active participants (Column 9, Lines 54-67). Wiser et al. does not explicitly disclose multicasting a message to said list of active participants, said message including a new key for use in decrypting a subsequent segment of said program content. Kandansky et al. discloses multicasting a message to said list of active participants, said message including a new key for use in decrypting a subsequent segment of said program content (Column 4, Lines 34-37). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky et al. in conjunction with the teachings of Wiser et al. for the benefit of disseminating data to a large group of receivers in a network (Column 1, Lines 9-10). The motivation for doing so is that when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key (Column 1, Lines 38-41).

As per **claim 25**, Wiser et al. discloses: providing a packet for use as an RTP packet comprising a header portion (Column 7, Lines 30-33, Column 16, Lines 14-21 and Column 24, Lines 21-23). Wiser et al. does not explicitly disclose: RTP packet comprising a payload header and inserting a field in said RTP packet operable to indicate key changes to said client so as to create a modified RTP packet. Kandansky et al. discloses (Column 9, Lines 62-67 and Column 10, Lines 1-5); transmitting said modified RTP packet to said client (Column 4, Lines 33-36). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky et al. in conjunction with the teachings of Wiser et al. for the benefit of disseminating data to a large group of receivers in a network (Column 1, Lines 9-10). The motivation for doing so is that when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key (Column 1, Lines 38-41).

As per **claim 29**, Wiser et al. discloses: providing a packet for use as an RTP packet comprising a header portion (Column 7, Lines 30-33 and Column 16, Lines 14-21 and Column 24, Lines 21-23). Not explicitly disclosed is utilizing a padding bit in said header portion to indicate key changes to said client. Kandansky et al. discloses utilizing a padding bit in said header portion to indicate key changes to said client (Column 7, Lines 25-30). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky et al. in conjunction with the teachings of Wiser et al. for the benefit of disseminating data

to a large group of receivers in a network (Column 1, Lines 9-10). The motivation for doing so is that when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key (Column 1, Lines 38-41).

As per **claim 2**, rejected as applied to claim 1. The combined references Wiser et al. and Kandansky et al. substantially teach receiving a request for a key from a client; logging said request for said key in a log; distributing said key to said client in response to said request; multicasting program content for decryption by said client utilizing said key; billing said client based upon said log. Furthermore, Wiser et al. discloses: not monitoring whether said client requires said key prior to said receiving said request for said key (Column 9, Lines 25-37).

As per **claim 3**, rejected as applied to claim 1. The combined references Wiser et al. and Kandansky et al. substantially teach receiving a request for a key from a client; logging said request for said key in a log; distributing said key to said client in response to said request; multicasting program content for decryption by said client utilizing said key; billing said client based upon said log. Furthermore, Wiser et al. discloses: logging a segment of said program content, wherein said key is used for decrypting said segment (Column 9, Lines 32-34 and Column 20, Lines 10-22).

As per **claim 4**, rejected as applied to claim 1. The combined references Wiser et al. and Kandansky et al. substantially teach receiving a request for a key from a client; logging said request for said key in a log; distributing said key to said client in response to said request; multicasting program content for decryption by said client

utilizing said key; billing said client based upon said log. Furthermore, Wiser et al. discloses: said key is encrypted under a program segment key and wherein said program segment key is distributed to said client in a multicast message (Column 9, Lines 25-36).

As per **claim 5**, rejected as applied to claim 4. The combined references Wiser et al. and Kandansky et al. substantially teach the method as described in claim 1 wherein said key is encrypted under a program segment key and wherein said program segment key is distributed to said client in a multicast message. Furthermore, Wiser et al. discloses: distributing said program segment key as part of a unicast message (Column 9, Lines 25-36).

As per **claim 6**, rejected as applied to claim 5. The combined references Wiser et al. and Kandansky et al. substantially teach The method as described in claim 4 wherein said distributing said program segment key to said client comprises: distributing said program segment key as part of a unicast message. Furthermore, Wiser et al. discloses: said program segment key is encrypted under a unique key of said client (Column 9, Lines 30-32).

As per **claim 7**, rejected as applied to claim 4. The combined references Wiser et al. and Kandansky et al. substantially teach the method as described in claim 1 wherein said key is encrypted under a program segment key and wherein said program segment key is distributed to said client in a multicast message. Furthermore, Kandansky et al. discloses: distributing said program segment key as part of a multicast message (Column 4, Lines 15-20). Therefore it would have been obvious to one with

ordinary skill in the art at the time the invention was made to use the teachings of Kandansky et al. in conjunction with the teachings of Wiser et al. for the benefit of disseminating data to a large group of receivers in a network (Column 1, Lines 9-10).

As per **claim 8**, rejected as applied to claim 7. The combined references Wiser et al. and Kandansky et al. substantially teach the method as described in claim 4 wherein said distributing said program segment key to said client comprises: distributing said program segment key as part of a multicast message. Furthermore, Wiser et al. discloses: said program segment key is encrypted under a unique key of said client (Column 9, Lines 30-32).

As per **claim 9**, rejected as applied to claim 4. The combined references Wiser et al. and Kandansky et al. substantially teach the method as described in claim 1 wherein said key is encrypted under a program segment key and wherein said program segment key is distributed to said client in a multicast message. Furthermore, Wiser et al. discloses: said client is a subscriber to a service and wherein said program segment key is encrypted under a service key (Column 9, Lines 25-37 and Column 10, Lines 18-29).

As per **claim 10**, rejected as applied to claim 9. The combined references Wiser et al. and Kandansky et al. substantially teach the method as described in claim 4 wherein said client is a subscriber to a service and wherein said program segment key is encrypted under a service key. Furthermore, Wiser et al. discloses: said service key is distributed to said client in response to said user purchasing said service associated with said service key (Column 9, Lines 25-37 and Column 10, Lines 18-29).



As per **claim 11**, rejected as applied to claim 10. The combined references Wiser et al. and Kandansky et al. substantially teach the method as described in claim 9 wherein said service key is distributed to said client in response to said user purchasing said service associated with said service key. Furthermore, Wiser et al. discloses: service key is encrypted under a unique key of said client (Column 9, Lines 30-32).

As per **claim 23**, rejected as applied to claim 22. The combined references Wiser et al. and Kandansky et al. substantially teach multicasting encrypted program content; creating a list of active participants receiving said program, said list of active participants including said client; receiving a message from said client indicating that said client should remain on said list of active participants; multicasting a message to said list of active participants, said message including a new key for use in decrypting a subsequent segment of said program content. Furthermore, Wiser et al. discloses: said key is encrypted with a key unique to each of said participants listed in said list of participants (Column 9, Lines 30-32).

As per **claim 24**, rejected as applied to claim 22. The combined references Wiser et al. and Kandansky et al. substantially teach multicasting encrypted program content; creating a list of active participants receiving said program, said list of active participants including said client; receiving a message from said client indicating that said client should remain on said list of active participants; multicasting a message to said list of active participants, said message including a new key for use in decrypting a subsequent segment of said program content. Furthermore, Kandansky et al. discloses: removing a second client from said list of active participants if a message

Art Unit: 2131

indicating that said second client should be maintained on said second list of participants is not received from said second client (Column 1, lines 38-43). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky et al. in conjunction with the teachings of Wiser et al. for the benefit of when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key (Column 1, Lines 38-41).

As per **claim 26, 27 and 28**, rejected as applied to claim 25. The combined references Wiser et al. and Kandansky et al. substantially teach providing a packet for use as an RTP packet comprising a payload portion and a header portion; inserting a field in said RTP packet operable to indicate key changes to said client so as to create a modified RTP packet; transmitting said modified RTP packet to said client.

Furthermore, Kandansky et al. discloses: receiving said modified RTP packet at said client (Column 5, Lines 15-17); removing said fixed field portion from said modified RTP packet so as to recover said RTP packet (Column 5, Lines 15-17); and determining from said fixed field portion whether a key change occurred (Column 7, Lines 42-53).

Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky et al. in conjunction with the teachings of Wiser et al. for the benefit of when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key (Column 1, Lines 38-41).

4. **Claims 12** is rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al. (U.S. Patent No. 6,385,596) in view of Kandansky et al. (U.S. Patent No. 6,295,361) in further view of Farris et al. (U.S. Patent No. 5,642,418).

**Claim 12** is rejected as applied to claim 1. The combined references Wiser et al. and Kandansky et al. substantially teach receiving a request for a key from a client; logging said request for said key in a log; distributing said key to said client in response to said request; multicasting program content for decryption by said client utilizing said key; billing said client based upon said log. Not explicitly disclosed is distributing a next content key in a first message wherein said next content key is encrypted under a first program segment key; distributing said next content key in a second message wherein said next content key is encrypted under a second program segment key; wherein said next content key is operable for decrypting a subsequent segment of said program content. However, Farris et al. discloses: distributing a next content key in a first message wherein said next content key is encrypted under a first program segment key (Column 4, Lines 50-65; distributing said next content key in a second message wherein said next content key is encrypted under a second program segment key (Column 4, Lines 66-67, Column 5, Lines 1-5); wherein said next content key is operable for decrypting a subsequent segment of said program content (Column 5, Lines 7-19). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Farris et al. in conjunction with the

Art Unit: 2131

combined references Wiser et al. and Kandansky et al. for the benefit preventing reception and display by unauthorized receiver units (Column 2, Lines 9-10).

5. **Claims 13, 14, 15, 20, 21, 30 and 32** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al. (U.S. Patent No. 6,385,596) in view Masuda et al. (EP 0969667 A2).

As per **claim 13**, Wiser et al. discloses: receiving from a client a request for a first key (Column 9, Lines 25-27, Line 57); creating a list of clients that request said first key (Column 18, Lines 23-29); and receiving a confirmation message from said client confirming that said client received said first key (Column 8, Lines 1-10). Not explicitly disclosed is distributing a multicast message to said list of clients that requested said first key so as to distribute a second key, wherein said second key is for use in decrypting encrypted program content. Masuda et al. disclose: distributing a multicast message to said list of clients that requested said first key so as to distribute a second key, wherein said second key is for use in decrypting encrypted program content (paragraph 15, Lines 1-8). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Masuda et al. in conjunction with the teachings of Wiser et al. for the benefit of reducing the loss due to illegal use of broadcast programs.

As per **claim 30**, Wiser et al. discloses: providing a first key for use by a first client (Column 9, Lines 25-27 and Line 57); encrypting said first key (Column 9, Lines 25-35). Not explicitly disclosed is providing a second key for use by a second client;

Art Unit: 2131

encrypting said second key; combining said encrypted first key and said encrypted second key as part of a message; multicasting said message to said plurality of clients so as to allow said first client to obtain said encrypted first key and said second client to obtain said encrypted second key. Masuda et al. discloses: providing a second key for use by a second client (Paragraph 15, Lines 1-8); encrypting said second key (Paragraph 15, Lines 1-8); combining said encrypted first key and said encrypted second key as part of a message (Paragraph 15, Line 6-8); multicasting said message to said plurality of clients so as to allow said first client to obtain said encrypted first key and said second client to obtain said encrypted second key (Paragraph 15, Line 5). ). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Masuda et al. in conjunction with the teachings of Wiser et al. for the benefit of reducing the loss due to illegal use of broadcast programs.

As per **claim 14**, rejected as applied to claim 13. The combined references Wiser et al. and Masuda et al. substantially teach receiving from a client a request for a first key; creating a list of clients that request said first key; distributing a multicast message to said list of clients that requested said first key so as to distribute a second key, wherein said second key is for use in decrypting encrypted program content; and receiving a confirmation message from said client confirming that said client received said first key. Furthermore, Masuda et al. discloses: said second key is encrypted utilizing said first key for each of said clients on said list (Paragraph 15, Lines 1-4). Therefore, it would have been obvious to one with ordinary skill in the art at the time the

Art Unit: 2131

invention was made to use the teachings of Masuda et al. in conjunction with the teachings of Wiser et al. for the benefit of reducing the loss due to illegal use of broadcast programs.

As per **claim 15**, rejected as applied to claim 14. The combined references Wiser et al. and Masuda et al. substantially teach The method as described in claim 13 wherein said second key is encrypted utilizing said first key for each of said clients on said list. Furthermore, Wiser et al. discloses: said first key is encrypted under a unique key (Column 9, Lines 27-29).

As per **claim 20**, rejected as applied to claim 13. The combined references Wiser et al. and Masuda et al. substantially teach receiving from a client a request for a first key; creating a list of clients that request said first key; distributing a multicast message to said list of clients that requested said first key so as to distribute a second key, wherein said second key is for use in decrypting encrypted program content; and receiving a confirmation message from said client confirming that said client received said first key. Furthermore, Wiser et al. discloses: billing said client based on the number of keys distributed to said client (Column 18, Lines 25-28). Not explicitly disclosed is repeatedly distributing new keys to said client. Masuda et al. discloses: repeatedly distributing new keys to said client (Paragraph 18, Lines 1-4). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Masuda et al. in conjunction with the teachings of Wiser et al. for the benefit of reducing the loss due to illegal use of broadcast programs.

As per **claim 21**, rejected as applied to claim 13. The combined references Wiser et al. and Masuda et al. substantially teach receiving from a client a request for a first key; creating a list of clients that request said first key; distributing a multicast message to said list of clients that requested said first key so as to distribute a second key, wherein said second key is for use in decrypting encrypted program content; and receiving a confirmation message from said client confirming that said client received said first key. Furthermore, Masuda et al. discloses: removing said client from said list after a confirmation message is not received within a predetermined period of time after said first key is distributed (Paragraph 18, Lines 1-4). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Masuda et al. in conjunction with the teachings of Wiser et al. for the benefit of reducing the loss due to illegal use of broadcast programs.

As per **claim 32**, rejected as applied to claim 30. The combined references Wiser et al. and Masuda et al. substantially teach providing a first key for use by a first client; encrypting said first key; providing a second key for use by a second client; encrypting said second key; combining said encrypted first key and said encrypted second key as part of a message; multicasting said message to said plurality of clients so as to allow said first client to obtain said encrypted first key and said second client to obtain said encrypted second key. Furthermore, Masuda et al. discloses: said first key and said second keys are program keys (Paragraph 15, Lines 4-5).

6. **Claims 16, 17, 18 and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al. (U.S. Patent No. 6,385,596) in view Masuda et al. (EP 0969667 A2) in further view of Kandansky et al (U.S. Patent No. 6,295,361).

As per **claim 16**, rejected as applied to claim 13. The combined references Wiser et al. and Masuda et al. substantially teach receiving from a client a request for a first key; creating a list of clients that request said first key; distributing a multicast message to said list of clients that requested said first key so as to distribute a second key, wherein said second key is for use in decrypting encrypted program content; and receiving a confirmation message from said client confirming that said client received said first key. Not explicitly disclosed is receiving a message from said client indicating that said client is leaving a multicast session. Kandansky et al. discloses: receiving a message from said client indicating that said client is leaving a multicast session (Column 1, Lines 38-39). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky in conjunction with the combined teachings of Wiser et al. and Masuda et al. for the benefit of when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key.

As per **claim 17**, rejected as applied to claim 16. The combined references Wiser et al., Masuda et al. and Kandansky et al. substantially teach the method as described in claim 13 and further comprising: receiving a message from said client indicating that said client is leaving a multicast session. Furthermore, Kandansky et al.



Art Unit: 2131

discloses: removing said client from said list (Column 1, Lines 38-43). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky in conjunction with the combined teachings of Wiser et al. and Masuda et al. for the benefit of when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key.

As per **claim 18**, rejected as applied to claim 16. The combined references Wiser et al., Masuda et al. and Kandansky et al. substantially teach the method as described in claim 13 and further comprising: receiving a message from said client indicating that said client is leaving a multicast session. Furthermore, Kandansky et al. discloses: in response to said receiving said message from said client, logging an entry indicating that billing of said client should be stopped for said multicast session (Column Column 18, Lines 23-29). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Kandansky in conjunction with the combined teachings of Wiser et al. and Masuda et al. for the benefit of when a member leaves a group or is no longer trusted, it is necessary to change the group key so that the former member will not be able to decrypt information encrypted with the group key.

As per **claim 19**, rejected as applied to claim 17. The combined references Wiser et al., Masuda et al. and Kandansky et al. substantially teach the method as described in claim 16 and further comprising: removing said client from said list. Furthermore, Masuda et al. discloses: distributing a third key to clients remaining on

Art Unit: 2131

said list so as to prevent said client removed from said list from being able to decrypt a subsequent segment of program content encrypted under said third key (Paragraph 15, Lines 1-8). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Masuda et al. in conjunction with the teachings of Wiser et al. for the benefit of reducing the loss due to illegal use of broadcast programs.

7. **Claim 31** is rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al. (U.S. Patent No. 6,385,596) in view Masuda et al. (EP 0969667 A2) in further view of Srivastava (U.S. Patent No. 6,684,331).

As per **claim 31**, rejected as applied to claim 30. The combined references Wiser et al. and Masuda et al. substantially teach providing a first key for use by a first client; encrypting said first key; providing a second key for use by a second client; encrypting said second key; combining said encrypted first key and said encrypted second key as part of a message; multicasting said message to said plurality of clients so as to allow said first client to obtain said encrypted first key and said second client to obtain said encrypted second key. Not explicitly disclosed is concatenating said encrypted first key and said encrypted second key in said message. However, Srivastava discloses concatenating said encrypted first key and said encrypted second key in said message (Column 18, Lines 57-67). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Srivastava in conjunction with the combined teachings of Wiser et al. and

Art Unit: 2131

Masuda et al. for the benefit of improved approach to distribution that enhances scalability and fault tolerance of group managers over a WAN, and the need for improved approaches for key updating (Column 4, Lines 55-60).

### ***Conclusion***

8. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sampat et al. (U.S. Patent No. 6,279,029) - Server/client for a network based multicast system.

Zhao et al. (U.S. Patent No. 6,141,753) - Secure distribution of digital representations with encryption and watermarking.


Art Unit: 2131

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saoussen Besrou who telephone number is 571-272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SB  
February 9, 2006

  
**AYAZ SHEIKH**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**